

Snort Installation Manual

Snort as a Slave Sensor



Windows NT4 Server, 2000, & XP
(All Versions)

Prepared & Written by Michael E. Steele
Technical Support Engineer for Silicon Defense
michaels@silicondefense.com
<http://www.silicondefense.com>

Document Version 1.1
Revised Date: Feb, 20, 2003
Silicon Defense
info@silicondefense.com
Phone: 707 445 4355
Fax: 707 445 4222

Table of Contents

Introduction	3
Copyright Notice	3
Disclaimer	3
Latest documentation & downloads	3
Comments & Corrections	3
Conceptual Topology	3
How to use this guide	4
Suggested prerequisites	4
Mandatory Prerequisites	4
Installing and configuring Snort	4
Installing WinPcap	5
Testing the Snort installation	6
Configuring Snort to run as a service	6
Explanation of the service options and commands	6
Configuring the Snort service	7
Modifying the MySQL database	7
Creating a remote Slave sensor database user	7
Testing the MySQL connection between the Slave and Master	8
Debugging Installation errors	9
Websites of interest	10
Revisions & Updates	10
Security tools & information	10

Introduction

This documentation will not only help understand how to install a Slave sensor using Snort that logs its unique alerts to a remote MySQL database, but guide you through the entire process, step by step.

When I set out to write this documentation, there was very little documentation for installing Snort for Windows. I have tried to make installing a full blown Intrusion Detection System using Snort in a Windows environment as painless as possible for the novice Windows user, and hopefully that is what I have done.

This guide includes all the necessary information and file linking's for installing an Intrusion Detection System, using Snort on a Windows box. It is **imperative** that the files in the links below are used in this installation, or the procedure may fail.

Copyright Notice

This document is Copyright © 2002-2003 Silicon Defense. All rights reserved. Permission to distribute this document is hereby granted providing that distribution is electronic, no money is involved, and this copyright notice is maintained. Other requests for distribution will be considered.

Disclaimer

Use the information in this document at your own risk. Silicon Defense disavows any potential liability of this document. Use of the concepts, examples, and/or other content of this document are entirely at your own risk.

This guide is written in the hope that it will be useful, but without any warranty; without even the implied warranty of merchantability or fitness for a particular purpose.

All copyrights are owned by their owners, unless specifically noted otherwise. Third party trademarks or brand names are the property of their owners. Use of a term in this document should not be regarded as affecting the validity of any trademark or service mark. Naming of particular products or brands should not be seen as endorsements.

Latest documentation & downloads

Latest up to date docs and files: <http://www.silicondefense.com/support/windows>

Comments & Corrections

If any errors that may be found or you would just like to make a comment please send them to: michaels@silicondefense.com

Conceptual Topology

There is only one primary software package that produces this topology, and that is Snort.

Snort: Snort is a lightweight network intrusion detection system, capable of performing real-time traffic analysis and packet logging on IP networks. This is the software package that is used to gather information from the network and send to the Master sensor.

Required Software

 [Snort 1.9.0 \(Build 229\) \(StdDB w/Service\)](#)

 [WinPcap 3.0 alpha4](#)

Note: We will be using WinRAR to uncompress any compressed files.

How to use this guide

This installation is based on a single slave sensor, interfacing to a single master sensor.

For this installation we started with a fresh install of XP with a single drive partitioned into 2 primary partitions (C & D). All programs and their subsystems will be installed on Drive 'D'.

This installation is based on the installer being logged on as 'Administrator' for the entire installation. Only the files downloaded from our website will be used. This installation may NOT work with either newer versions or lesser versions of the same program.

Suggested prerequisites

- Fresh install of Windows
- Hard Drive Partition C - Min 2 Gigabytes
- Hard Drive Partition D - Min 10+ Gigabytes
- All Service Packs and Patches applied

I would strongly suggest a clean install to start this installation, but it's certainly is not required. If this is being installed on a dirty disk then make SURE that, all Service Packs and Patches have been applied, ANY of these programs that are going to be installed, that have been previously installed, are COMPLETELY removed before starting this installation, especially WinPcap.

Mandatory Prerequisites

- The Master sensor must be completely setup using one of these instructions: [Apache](#) or [IIS](#)
- An unobstructed path between the Master & Slave sensor (ping each other).
- The hostname for the SLAVE & MASTER sensors must resolve to an IP address.

Installing and configuring Snort

- Navigate into the 'D:\' drive, and create a folder called 'Applications'. This folder will be the home location for all the support programs for this installation.
- Uncompress 'Snort_1.9.0b6-229_Win32_StdDB_Service_Release.zip' into the 'D:\Applications' folder.
- Navigate into the folder 'D:\Applications\snort', and create a folder called 'log'.
- Load the file 'D:\Applications\snort\etc\snort.conf' into WordPad. Several variables located in that file will need to be changed. Use the search routine to find and edit them.

Original: var HOME_NET any

Note: The IP and Subnet variables in the examples below are purely fictitious.

To monitor a single host, with an IP of 10.0.0.3
Change: var HOME_NET 10.0.0.3/32

To monitor a class C Network with an IP of 10.0.0.x, and a subnet of 255.255.255.x
Change: var HOME_NET 10.0.0.0/24

To monitor a class B network with an IP of 10.0.x.x, and a subnet of 255.255.x.x
Change: var HOME_NET 10.0.0.0/16

To monitor a class A Network with an IP of 10.x.x.x, and a subnet of 255.x.x.x
Change: var HOME_NET 10.0.0.0/8

Note: By default Snort will monitor the complete network using 'var HOME_NET any'

Note: There are several other settings that will need to be changed, and these MUST be copied EXACTLY as they are described here. Do a search and replace the like same lines.

Original: var RULE_PATH ../rules
Change: var RULE_PATH d:/applications/snort/rules

Original: # output database: log, mysql, user=root password=test dbname=db host=localhost
Change: output database: log, mysql, user=snort password=123 dbname=snort host=127.0.0.1
port=3306 sensor_name=SENSOR_NAME

Original: # output database: alert, postgresql, user=snort dbname=snort
Change: output database: alert, mysql, user=snort password=123 dbname=snort host=127.0.0.1
port=3306 sensor_name=SENSOR_NAME

Note: In the two output database lines above, there is a sensor_name=SENSOR_NAME. This SENSOR_NAME is usually the hostname of the sensor. This name is displayed in the Acid console when alerts are being viewed.

Original: # output alert_syslog: LOG_AUTH LOG_ALERT
Change: output alert_syslog: LOG_AUTH LOG_ALERT

Note: This will allow Snort to send alerts to the Application log located in the Event Viewer. If logging to the Application Log is not important, then leave the hash mark (#) in.

Original: include classification.config
Change: include d:/applications/snort/etc/classification.config

Original: include reference.config
Change: include d:/applications/snort/etc/reference.config

Now save the file and exit...

Installing WinPcap

- Double click on the 'WinPcap_3_0_a4.exe' file, and install using all defaults.

Testing the Snort installation

Navigate to 'D:\Application\snort'

- At the command prompt '>' type: snort -W

Note: If WinPcap is operating properly, and snort has been installed correctly, there will be a list of possible sniffing interfaces shown by a number. The correct interface **MUST** be selected or Snort will not detect traffic.

Note: The interface number that was derived using the 'Snort -W' switch, will be used throughout the next several exercises. The switch for designating a particular interface, is '-ix', and 'x' will always be the interface number that was derived by using the 'Snort -W' switch.

- At the command prompt '>' type: snort -v -ix

Note: This will run Snort in verbose mode (-v) on a specific interface (-ix). The 'x' in '-ix' is the number of the Network Interface Card that Snort will sniff on. If Snort is operating properly then packets should be streaming by in the command window, but if not, open a browser and surf the web and generate some traffic.

- At the command prompt '>' press the 'CTRL/C' keys to exit

Note: All errors must be resolved before continuing, see debugging installation errors!

Configuring Snort to run as a service

Note: If a Snort service was previously installed using the 'INSTSRV.exe' program, then that service **MUST** be removed, otherwise the built-in service installer for Snort will fail.

- To remove the service that was installed using "INSTSRV.EXE" and "SRVANY.EXE" you will need to stop the snort service.
- From a command prompt type (make sure INSTSRV is in the path):

```
"instsrv srvany remove"  
"instsrv snort remove"
```

- Start "REGEDIT.EXE" from the run box and locate and delete the following sub key:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Snort

Now reboot the system...

Explanation of the service options and commands

- There are three command switches that Snort uses for the Service activation.

Note: It is **IMPERATIVE** these commands **ALWAYS** be executed in the same folder as Snort.

```
/SERVICE /INSTALL  
/SERVICE /UNINSTALL  
/SERVICE /SHOW
```

Snort Installation Guide – *Windows NT4 Server / 2000 / XP*

This will install Snort as a service with the specified parameters:

```
snort /SERVICE /INSTALL -de -c c:/snort/snort.conf -l c:/snort/logs -ix
```

Note: -ix (x is the number of the NIC for Snort to sniff on)

Note: After every 'snort /SERVICE /INSTALL', be SURE to run the service applet, and set the 'snort' entry to 'Automatic', or the service will fail to start at a reboot.

This will remove snort as a service:

```
snort /SERVICE /UNINSTALL
```

This will display the parameters:

```
snort /SERVICES /SHOW
```

Starting and stopping Snort from a command prompt:

```
net stop snort or net start snort
```

Note: Snort can be stopped, started, and restarted from the Service applet.

Configuring the Snort service

- From a command prompt, navigate to the 'D:\Application\snort' folder and type:

```
snort /SERVICE /INSTALL -c d:/applications/snort/etc/snort.conf -l d:/applications/snort/log -ix
```

Note: -ix (x is the number of the NIC for Snort to sniff on)

Note: You should receive a confirmation that the service has successfully installed.

- Start the Services applet, either in the Windows 2000 or Windows XP Control Panel, or in the Administrative Tools folder located in the Control Panel.
- From the Services applet, scroll down, right click on the entry 'snort', select 'Properties', in the 'Startup Type' select 'Automatic', click the 'OK' button, and exit the Services applet.

Modifying the MySQL database

Note: These modifications will need to be done on the Master Sensor.

- Right click on the MySQL Admin module in the system tray and select 'Show Me'
- Select the 'my.ini Setup' tab

Original: bind-address=127.0.0.1

Change: (completely remove line)

- Click the 'Save Modification' button, click 'Yes', and click 'OK'.

Creating a remote Slave sensor database user

From a command prompt Navigate to the 'D:\Applications\mysql\bin' folder.

- At the command prompt '>' type:

```
mysql -u root -p
```

Note: At the password prompt enter the password of the pre-configured user 'root'.

- Note: It is IMPERATIVE that a semicolon is added as shown in the commands below.
- At the 'mysql>' prompt type: grant INSERT,SELECT on snort.* to snort1@HOST_NAME identified by "123";

Note: In the above 'grant' line, there is a snort1@HOST_NAME. This HOST_NAME must be the hostname of the 'slave sensor'.

- At the 'mysql>' prompt type: show grants for snort1@HOST_NAME;

Note: This should show the privileges for user 'snort1', and they should match what was added.

Now reboot your new IDS Master Sensor!

Note: Allow the Master sensor to come all the way up before continuing.

Now reboot your new IDS Slave Sensor!

Testing the MySQL connection between the Slave and Master

- From a command prompt on the Slave sensor type: telnet hostname 3306

Note: The 'hostname' must be the hostname of the Master sensor. If there is a clear path to the MySQL database there will be a good connect.

Note: All errors must be resolved before continuing, see debugging installation errors!

- If the webserver is IIS then go to the browser and type: <http://localhost/Console/Index.html>
- If the webserver is Apache then go to the browser and type: <http://localhost/acid/Index.html>

Note: Acid MUST always be initiated using the above commands from the browser:

Note: The ACID console will display each remote sensor as they are added. It may take a little while to start seeing alerts from the slave sensor, just let it go, and Acid will auto refresh.

Debugging Installation errors

As of Snort V 1.9.0 b229, Snort will now throw FATAL errors to the Event Viewer under the System log tab.

If there is no traffic moving, there are several possibilities.

- Wrong network card selected using the -i switch.
- Network card may need a driver update.
- A previously installed 'WinPcap' was not properly removed.
- No network connection.
- Snort does not operate on dual processors.
- Snort does not operate on a PPOE connection.
- If connected to a switch the ports must be mirrored.
- Ethernet card or cable not secure, or bad.

If there is a MySQL connection refused error, there are several possibilities.

- The 'my.ini' file has a 'bind-address=' line included.
- No clear path to Master sensor (firewall / switch).
- The Snort run line may be incorrect (make SURE -l is a lowercase L).

Websites of interest

Snort Home Page <http://www.snort.org/>
Snort FAQ <http://www.snort.org/docs/faq.html>
Snort Users Manual http://www.snort.org/docs/writing_rules/
Usenet Groups
 Snort-announce <http://lists.sourceforge.net/mailman/listinfo/snort-announce>
 Snort-users <http://lists.sourceforge.net/mailman/listinfo/snort-users>
 Snort-sigs <http://lists.sourceforge.net/mailman/listinfo/snort-sigs>
 Snort-devel <http://lists.sourceforge.net/mailman/listinfo/snort-devel>
 Snort-cvsinfo <http://lists.sourceforge.net/mailman/listinfo/snort-cvsinfo>
Snort CVS tree <http://cvs.sourceforge.net/cgi-bin/viewcvs.cgi/snort/snort/>
ACID Home Page <http://acidlab.sourceforge.net/>
MySQL Home Page <http://www.mysql.com/>
PHP Home Page <http://www.php.net>
WinPcap Home Page <http://winpcap.polito.it/>

Revisions & Updates

V1.0 Feb 4, 2003
 Initial 1.9.x document in HTML format

V1.1 Feb 20, 2003
 Initial 1.9.x document converted to PDF
 Update PHP (security Fixes)
 Update MySQL to 4.0.10 (minor)
 Update Snort to b229 (Fatal errors to Event Log)

Security tools & information

XP Security Checklist <http://www.labmice.net/articles/winxpsecuritychecklist.htm>
NSA Securing XP <http://nsa1.www.conxion.com/winxp/guides/wxp-1.pdf>

Michael E. Steele | System Engineer / Support Technician
Email Me: <mailto:michaels@silicondefense.com>
Commercial Snort Support - 1.866.41.SNORT
Silicon Defense - **The Cyber-War Defense Company**
Our Website - <http://www.silicondefense.com>
Snort: Open Source Network IDS - <http://www.snort.org>